UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

# NOTICE OF ALLOWANCE AND FEE(S) DUE

22879 7590 09/01/2009

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

| EXAMINER | |
|---|---|
| GEROTSO, TECHANE | |
| ART UNIT | PAPER NUMBER |
| 2437 | |

DATE MAILED: 09/01/2009

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/825,596 | 04/14/2004 | Cheh Goh | 300111166-4 | 7793 |

TITLE OF INVENTION: SECURE DATA PROVISION METHOD AND APPARATUS AND DATA RECOVERY METHOD AND SYSTEM

| APPLN. TYPE | SMALL ENTITY | ISSUE FEE DUE | PUBLICATION FEE DUE | PREV. PAID ISSUE FEE | TOTAL FEE(S) DUE | DATE DUE |
|---|---|---|---|---|---|---|
| nonprovisional | NO | $1510 | $300 | $0 | $1810 | 12/01/2009 |

**THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.**

**THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.**

**HOW TO REPLY TO THIS NOTICE:**

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

**IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.**

## PART B - FEE(S) TRANSMITTAL

**Complete and send this form, together with applicable fee(s), to: Mail** **Mail Stop ISSUE FEE**
**Commissioner for Patents**
**P.O. Box 1450**
**Alexandria, Virginia 22313-1450**
**or Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22879 7590 09/01/2009

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/825,596 | 04/14/2004 | Cheh Goh | 300111166-4 | 7793 |

TITLE OF INVENTION: SECURE DATA PROVISION METHOD AND APPARATUS AND DATA RECOVERY METHOD AND SYSTEM

| APPLN. TYPE | SMALL ENTITY | ISSUE FEE DUE | PUBLICATION FEE DUE | PREV. PAID ISSUE FEE | TOTAL FEE(S) DUE | DATE DUE |
|---|---|---|---|---|---|---|
| nonprovisional | NO | $1510 | $300 | $0 | $1810 | 12/01/2009 |

| EXAMINER | ART UNIT | CLASS-SUBCLASS |
|---|---|---|
| GERGISO, TECHANE | 2437 | 713-161000 |

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☐ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/825,596 | 04/14/2004 | Cheh Goh | 300111166-4 | 7793 |

22879 7590 09/01/2009

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

| EXAMINER | |
|---|---|
| GERGISO, TECHANE | |
| ART UNIT | PAPER NUMBER |
| 2437 | |

DATE MAILED: 09/01/2009

**Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)**
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 1010 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 1010 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

| Notice of Allowability | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/825,596 | GOH ET AL. | |
| | Examiner | Art Unit | |
| | TECHANE J. GERGISO | 2437 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--***

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *06/02/2009*.

2. ☒ The allowed claim(s) is/are *23-28 and 43-58*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   **Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

## DETAILED ACTION

1. This is a notice of allowance in response to the applicant's communication filed on June 02, 2009.

## EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

3. The applicant's representative David Millers (Reg. No.: 37,396) gave authorization for the following examiner's amendment on August 21, 2009.

The application has been amended as follows:

Listing of Claims:

Claims 1-22. (Cancelled).

23. (Currently Amended) A secure data-provision method for providing target data from a data provider to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organization, the target data being provided in encrypted form as part of a data set; the method comprising:

encrypting a first item, ~~according to~~ by a processor executing an Identifier-Based Encryption, IBE, scheme, in dependence on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations; and

encrypting a second item, ~~according to~~ by a processor executing an IBE scheme, in dependence on encryption parameters comprising a second encryption key string that identifies said specific organization, and public data of a second trusted authority competent in respect of accreditations of organizations; and

forming said data set using at least the encrypted first and second items;

recovery of the target data in clear requiring decryption of both the first and second items.

24. (Currently Amended) The [[A]] method according to claim 23, wherein the first item comprises the target data, and the second item comprises the encrypted first item.

25. (Currently Amended) The [[A]] method according to claim 23, wherein the first item comprises the target data, and the second item comprises a nonce; the first encryption key string comprising, in combination, an identifier of said specific individual and said nonce.

26. (Currently Amended) The [[A]] method according to claim 23, wherein the first item comprises first data, and the second item comprises second data; the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data.

27. (Currently Amended) The [[A]] method according to claim 23, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key.

28. (Currently Amended) A secure data-provision method for providing target data from a data provider to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organization, the target data being provided in encrypted form as part of a data set, the method comprising:

encrypting a first item by a processor using both a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations; and

encrypting a second item by a processor using both a second encryption key string that identifies said specific organization, and public data of a second trusted authority competent in respect of accreditations of organizations; and

forming said data set using at least the encrypted first and second items;

recovery of the target data in clear requiring decryption of both the first and second items.

Claims 29-42. (Cancelled).

43. (Currently Amended) An apparatus for the secure provision of target data to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organization, the apparatus comprising:

[[an]] a processor encryption subsystem for generating a data set including the target data in encrypted form; ~~, the encryption subsystem comprising:~~

first encryption means for encrypting a first item, according to an Identifier-Based Encryption, IBE, scheme, based on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations;

second encryption means for encrypting a second item, according to an IBE scheme, based on encryption parameters comprising a second encryption key string that identifies said specific organization, and public data of a second trusted authority competent in respect of accreditations of organizations; and

means for forming the data set using at least the encrypted first and second items; the recovery of the target data in clear requiring decryption of both the first and second items.

44. (Currently Amended) The apparatus according to claim 43, wherein the first item comprises the target data, and the second item comprises the encrypted first item.

45. (Currently Amended) The apparatus according to claim 43, wherein the first item comprises the target data, and the second item comprises a nonce; the first encryption key string comprising, in combination, an identifier of said specific individual and said nonce.

46. (Currently Amended) The apparatus according to claim 43, wherein the first item comprises first data, and the second item comprises second data; the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data.

47. (Currently Amended) The apparatus according to claim 43, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key.

48. (Currently Amended) A computing entity for recovering target data provided in encrypted form as part of an data set that comprises first and second encrypted items both of which must be decrypted to recover the target data, the first item being encrypted in dependence on encryption parameters comprising a first encryption key string that identifies a specific individual and first public data, and the second item being encrypted in dependence on a second encryption key string that identifies a specific organization and second public data; the entity comprising:

a processor-based system comprising;

first means for requesting either a first decryption key corresponding to the first encryption key string, or the first item in decrypted form, from a first trusted authority and holds first private data related to the first public data, the first means being arranged to provide the first encryption key string to the first trusted authority when making its request and being further arranged to authenticate the entity with the first trusted authority and to receive the first decryption key, or the first item, securely from the first trusted authority;

second means for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, from an organization accredited by a second trusted authority which holds second private data related to the second public data, the second means being arranged to provide the second encryption key string to the organization when making its request and being further arranged to authenticate the entity with the organization and receive the second decryption key, or the second item, from the organization;

third means for using the first decryption key, or the first item, provided by the first trusted authority and the second decryption key, or the second item, provided by the organization, to recover the target data.

49. (Currently Amended) The [[A]] computing entity according to claim 48, wherein the second means is arranged to receive the second decryption key, or the second item, securely from the organization.

50. (Currently Amended) The [[A]] computing entity according to claim 48, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the third means being arranged to recover the second item, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization, and subject the second item to decryption, using the first decryption key obtained from the first trusted authority, to recover the target data (0077; 0082).

51. (Currently Amended) The [[A]] computing entity according to claim 48, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the third means being arranged to: recover the second item, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization, combine the nonce that formed the second item with the identifier of said specific individual in order to form the first encryption key string to be provided by the first means to the first trusted authority and use the first decryption key obtained from the first trusted authority to decrypt the first item and thereby recover the target data.

52. (Currently Amended) The [[A]] computing entity according to claim 48, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the third means being arranged to recover the first data, if not provided to the first means by the first trusted authority, by using the first decryption key

obtained from the first trusted authority, recover the second data, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization, use the first data and the second data to form said symmetric key, and use the symmetric key to decrypt the target data.

53. (Currently Amended) The [[A]] computing entity according to claim 48, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the third means being arranged to: recover the first item, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority, recover the second item, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization, use the second symmetric key that formed the second item to decrypt the encrypted first symmetric key that formed the first item, and use the first symmetric key to decrypt the encrypted target data.

54. (Currently Amended) A computing entity for recovering target data provided in encrypted form as part of an data set that comprises first and second encrypted items both of which must be decrypted to recover the target data; the first item being encrypted in dependence on a first encryption key string that identifies a specific individual, and first public data; and the second item being encrypted in dependence on a second encryption key that identifies a

specific organization and said specific individual, and second public data; the entity comprising:

a processor-based system comprising;

first means for requesting either a first decryption key corresponding to the first encryption key, or the first item in decrypted form, from a first trusted authority which is competent in respect of the accreditation of professionals and holds first private data related to the first public data, the first means being arranged to provide the first encryption key string, or the first item, to the first trusted authority when making its request;

second means for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, from an organization accredited by a second trusted authority which holds second private data related to the second public data, the second means being arranged to provide the second encryption key string to the organization when making its request; and

third means for using the first decryption key, or the first item, provided by the first trusted authority and the second decryption key, or the second item, provided by the organization, to recover the target data;

at least one of the first means and the second means being arranged to authenticate the entity to the first trusted authority or said organization as the case may be and to receive input therefrom in a secure manner.

55. (Currently Amended) The [[A]] computing entity according to claim 54, wherein computing entity, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the third means being arranged to: recover the second item, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization, and subject the second item to decryption, using the first decryption key obtained from the first trusted authority, to recover the target data (0077; 0082).

56. (Currently Amended) The [[A]] computing entity according to claim 54, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the third means being arranged to: recover the second item, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization, combine the nonce that formed the second item with the identifier of said specific individual in order to form the first encryption key string to be provided by the first means to the first trusted authority, and use the first decryption key obtained from the first trusted authority to decrypt the first item and thereby recover the target data.

57. (Currently Amended) The [[A]] computing entity according to claim 54, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the third means being arranged to recover the first data, if not

provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority, recover the second data, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization, use the first data and the second data to form said symmetric key, and use the symmetric key to decrypt the target data.

58. (Currently Amended) The [[A]] computing entity according to claim 54, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the third means being arranged to: recover the first item, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority, recover the second item, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization, use the second symmetric key that formed the second item to decrypt the encrypted first symmetric key that formed the first item, and use the first symmetric key to decrypt the encrypted target data.

## Reason for allowance

4. After consideration of the appellant's argument filed on June 02, 2009 in response to the Final Office Action mailed on January 07, 2009, and through examination of claims 23-28 and

43-58 with respect to the prior arts in record during the appeal conference and proposed examiner's amendment, the claims have been found in condition for allowance.

5. The following is an examiner's statement of reasons for allowance:

Claims 23 and 43 include the following features of a method and apparatus which are not taught or further suggested and would not have been obvious over prior arts of record and these claimed features are: encrypting a first item of a data set based on Identifier-Based Encryption scheme using a first encryption key string that identifies a specific individual and public data of a first trusted authority associated with a professional accreditations; encrypting a second item of a data set based on Identifier-Based Encryption scheme using a second encryption key string that identifies a specific organization and public data of a second trusted authority associated with accreditations of organizations; and forming said data set using at least the encrypted first item and second items.

Claim 28 includes the following features of a method which are not taught or further suggested and would not have been obvious over prior arts of record and these claimed features are: encrypting a first item of a data set using a first encryption key string that identifies a specific individual and public data of a first trusted authority associated with a professional accreditations; encrypting a second item of a data set using a second encryption key string that identifies a specific organization and public data of a second trusted authority associated with accreditations of organizations; and forming said data set using at least the encrypted first item and second items.

Claim 48 and 54 include the following features of computing entity which are not taught or further suggested and would not have been obvious over prior arts of record and these claimed features are: encrypting a first item of a data set using a first encryption key string that identifies a specific individual and public data of a first trusted authority associated with a professional accreditations; encrypting a second item of a data set using a second encryption key string that identifies a specific organization and public data of a second trusted authority associated with accreditations of organizations. The first means being arranged to provide the first encryption key string to the first trusted authority when making its request and arranged to authenticate the entity with the first trusted authority and to receive the first decryption key, or the first item, securely from the first trusted authority; the second means being arranged to provide the second encryption key string to the organization when making its request and arranged to authenticate the entity with the organization and receive the second decryption key, or the second item, from the organization.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

## Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior art.

## Contact Information

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is **(571) 273-3784**. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Techane J. Gergiso/

Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437